A Report on
Five Day National Level Online Faculty Development Programme on "Leveraging AI: Human Factors in Cyber Security"
Organized by Department of Computer Science & Engineering (Cyber Security)
in Association with IEEE Student Branch
From 08.07.2024 to 12.07.2024

Submitted by: Dr. KP Manikandan, Assistant Professor / CSE (CS)
Coordinators: Dr. KP Manikandan, Assistant Professor / CSE (CS), Mrs. M Srilakshmi Preethi, Assistant Professor / CSE (CS)

Resource persons:

Date: 08.07.2024

Session: I - Dr D. PAULRAJ, Professor, R.M.K Engineering College, Chennai
Session: II -Ms. Guntur Renu Chief Operating Officer (COO) of KanProKaGno Pvt. Ltd

Date: 09.07.2024
Session: I – Dr Vijayanand, Associate Professor, Vel Tech University, Avadi
Session: II - Dr. Kennedy Babu, Professor, Saveetha School of Engineering

Date: 10.07.2024
Session: I - Dr. Konatham Sumalatha, Assistant Professor, VIT Vellore.
Session: II - Mrs. M. Srilakshmi Preethi, Assistant Professor, MITS, Madanapalle
Date: 11.07.2024
Session: I - Mr. Saketh Gundlapalli, Senior DevOps Engineer Nowtilus GmBH, Germany
Session: II - Mrs.Thalla Radhika, Assistant Professor, Vignana Jyothi institute of arts and sciences, Hyderabad.

Date: 12.03.2024
Session: I - Mrs.A.Komala, Assistant Professor ,MITS , Madanapalle.

Mode of conduct: Online

Report Received on 24.07.2024

Total Participants: 110 Faculties from various institutions.

About the FDP:

The program aims to provide insights into core research issues and hands-on training in identifying appropriate research problems for integrating Cyber Security and its applications. This program addresses the research and applications explores the interplay between AI and human elements in cybersecurity, highlighting key areas where human factors can either enhance or undermine security efforts.

The primary goal of this Faculty Development Programme (FDP) is to provide comprehensive knowledge on in the Common Factors in Cyber Security to faculty members.

Inaugural Session:

The Department of Computer Science & Engineering (Cyber Security) successfully hosted a Five-Day National Level Online Faculty Development Program titled " **Leveraging AI: Human Factors in Cyber Security"** from July 08 to July 12, 2024. This esteemed initiative was executed through an online platform, drawing a remarkable attendance of 110 participants nationwide.

The Faculty Development Program commenced at 10:00 AM on July 08. Dr.KP Manikandan, Coordinator has given the opening remarks about the FDP programme and Welcomed all Dignitaries, Head of the Department / CSE(CS), Chief guest and Resource person and all the external participants and highlighted the institute achievements and facilities. Totally we received 110 registrations from various institutions.

Dr. S V S Ganga Devi, HoD CSE(CS), graced the occasion with a felicitation address, adding an impression of significance to the event. Her presence and spoken words brought gravitas to the proceedings. She extended his best wishes to all participants, advise them to actively participate in the FDP and embrace new knowledge and insights.

Following the HoD speech, Mrs M Srilakshmi Preethi, Coordinator, extended a cordial and insightful welcome to all attendees. In her address, she highlighted the programme's importance of Cyber Security in the current environment and welcome the Resource Person.

Date: 08.07.2024 Session: I - Dr D. PAULRAJ, Professor, R.M.K Engineering College, Chennai

Dr D. PAULRAJ delivered talk in the title of "**Introduction to AI in Cyber Security**" and he started with the Artificial Intellilance basics and he discussed about various challenges and solutions through Image Processing techniques in the field of medical industry.

His lecture was very informative to the participants and given more insights on composites.
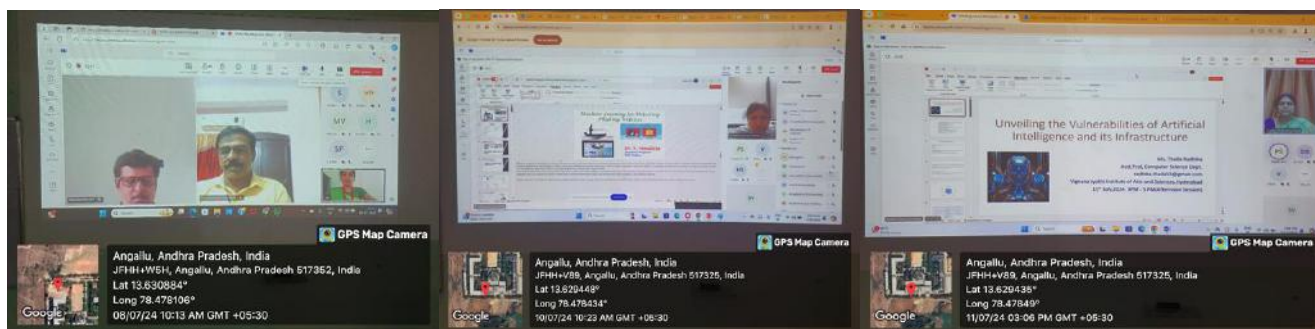
Date: 08.07.2024 Session: II – Ms. Guntur Renu Chief Operating Officer (COO) of KanProKaGno Pvt. Ltd

Ms. Guntur Renu delivered talk in the title of "**Privacy Awareness in ML**" and she explained about the organization of contents expressed.

Date: 09.07.2024 Session: I – Dr Vijayanand, Associate Professor, Vel Tech University, Avadi

Dr Vijayanand delivered talk in the title of "**Cyber Threat Intelligence**" and He discussed about the types of threats. He provided the hands-on demo on securing the data with the using of Artificial Intelligence.

Date: 09.07.2024 Session: II - Dr. Kennedy Babu, Professor, Saveetha School of Engineering

Dr. Kennedy Babu delivered talk in the title of "**AI for Cybercrime Investigation and Forensics**" and He discussed about the basics of cyber security and its current challenges. He provided the hands-on demo on Real time attacks monitoring and control strategies.

Date: 10.07.2024 Session: I - Dr. Konatham Sumalatha, Assistant Professor, VIT Vellore.

Dr. Konatham Sumalatha delivered talk in the title of "**Machine Learning for Detecting Phishing Websites**" and She discussed about the Feature Extraction basics and its types. She also expressed her research problems and solutions.

Date: 10.07.2024 Session: II - Mrs. M. Srilakshmi Preethi, Assistant Professor, MITS, Madanapalle.

Mrs. M. Srilakshmi Preethi delivered talk in the title of "**Machine Learning-Based Techniques for Network Intrusion Detection**" and She discussed about the various Intrusion types, challenges and solutions. She provided the hands-on demo.

Date: 11.07.2024 Session: I - Mr. Saketh Gundlapalli, Senior DevOps Engineer Nowtilus GmBH, Germany

Mr. Saketh delivered talk in the title of "**Big Data and Data Science for Security and Fraud Detection**" and he discussed about the various Data Analytical tools and their features. he expressed her research problem and solution in Teaching and Learning are with the use of data filter tools.

Date: 11.07.2024 Session: II – Mrs.Thalla Radhika, Assistant Professor, Vignana Jyothi institute of arts and sciences, Hyderabad.

Mrs.Thalla Radhika delivered talk in the title of "**Vulnerabilities of AI Infrastructure**" and She discussed about the fundamentals and methods. She also expressed his research problems and solution by using the various vulnerability methods.

Date: 12.07.2024 Session: I - Mrs. A. Komala, Assistant Professor ,MITS , Madanapalle.

Mrs A Komala delivered talk in the title of "**Pedagogy**" and She discussed about the various types and challenges and Artificial Intelligence basics. Shee given real examples and conducted practice session

Valedictory Ceremony:

Mrs M Srilakshmi Preethi, Coordinator, Dept. of CSE(CS), MITS anchored the valedictory ceremony. Dr.Kamal Basha, Vice Principal (Administration) ,addressed in the valedictory ceremony meeting and briefed about the summary of the College and support from Management, Dr S V S ganga Devi, Head of the Department explored a summary of the FDP program. Few participants shared their experience and highlighted the FDP. Dr. KP Manikandan, Coordinator, Dept. of CSE(CS), thanked all the participants for providing support and attending the 5 Day programme.

Outcome of the FDP:

The Faculty Development Program (FDP) on "Leveraging AI: Human Factors in Cyber Security" aims to equip participants with comprehensive knowledge and practical skills at the intersection of artificial intelligence and human factors in cybersecurity. Upon completion of this program, participants can expect to achieve the following outcomes:

1. Enhanced Understanding of AI in Cybersecurity:

Participants will gain a deep understanding of how AI technologies, such as machine learning and predictive analytics, are transforming cybersecurity practices. They will learn how AI can be applied to various aspects of cybersecurity, including threat detection, risk assessment, and incident response

2. Awareness of Human Factors:

The program will highlight the critical role of human factors in cybersecurity. Participants will explore how user behavior, organizational culture, and decision-making processes impact security and how these factors can be managed to enhance overall cybersecurity posture.

3. Improved Skills in Integrating AI with Human Elements:

Participants will develop practical skills to effectively integrate AI solutions with human elements in cybersecurity strategies. This includes understanding the concept of augmented intelligence, where AI supports human decision-making, and learning to design adaptive learning systems that evolve with new threats.

4. Hands-on Experience with AI Tools:

Through practical sessions and labs, participants will gain hands-on experience with AI tools and technologies used in cybersecurity. This practical exposure will enable them to apply AI-driven solutions in real-world scenarios and understand the limitations and potential of these technologies.

5. Strategies for Building a Strong Security Culture:

The program will provide insights into building and maintaining a robust security culture within organizations. Participants will learn best practices for fostering a security-conscious environment, conducting effective training and awareness programs, and encouraging proactive security behaviors among employees.

6. Knowledge of Ethical and Bias Considerations:

Participants will be educated on the ethical considerations and potential biases in AI systems. They will learn how to identify and mitigate biases in AI algorithms to ensure fair and unbiased security measures.

7. Enhanced Decision-Making Capabilities:

Participants will enhance their decision-making capabilities by learning how to interpret AI-generated insights and make informed decisions in complex or ambiguous cybersecurity situations.

8. Networking and Collaboration Opportunities:

The FDP will provide a platform for participants to network with peers, industry experts, and thought leaders in the field of cybersecurity and AI. This collaboration will foster the exchange of ideas and best practices, contributing to ongoing professional development

Conclusion:

By the end of the Faculty Development Program on "Leveraging AI: Human Factors in Cyber Security," participants will be well-equipped to address the challenges and opportunities at the intersection of AI and human factors in cybersecurity. They will possess the knowledge, skills, and strategies needed to create more resilient and adaptive cybersecurity frameworks in their respective organizations or institutions.